Hewlett Packard
Enterprise

Data sheet

HPE SecureMail Add-Ons

Offer integration with your business workflow that includes employees, partner communities, and customers

Highlights

- Simple and convenient access to encrypted email via mobile devices
- Rapid access to secure email for eDiscovery and archiving
- Advanced secure messaging add-ons that align to and enable business processes

HPE SecureMail uses proven encryption technologies that provide powerful security for even the most sensitive email communications. Compared to competing solutions, it is the easiest to manage and use. HPE SecureMail can help you meet and maintain regulatory compliance, and enforce best practice email protection, without disrupting business. It reduces the risk of email security breaches by giving you end-to-end email encryption—including mobile devices. HPE SecureMail will integrate smoothly with your existing infrastructure. And it can be rapidly deployed—both internally and externally—organizations of any size. Besides the proven HPE SecureMail core capabilities, a range of robust enterprise-class features is available for HPE SecureMail, to enhance its capabilities.

Extend compliance and business to leading mobile platforms

HPE SecureMail Mobile Edition allows employees, partners, and customers to read and send HPE SecureMail encrypted email on support iOS, Android, and Blackberry devices—with advanced mobile policy control. The solution extends data-centric protection and compliance to mobile email messages and attachments with a simple, anywhere, anytime native-user experience. Businesses of all sizes can unlock full, rich mobile policies and native app capabilities, delivering immediate value and enhancing HPE SecureMail deployments. The mobile apps work with existing email client applications—without requiring an additional secure mobile inbox or webmail service. Users enjoy the familiar email experience and native phone features for ease of use and convenience. HPE SecureMail Mobile Edition significantly enhances Mobile Device Management (MDM) device-level controls—protecting email messages and attachments wherever they go—even externally to customers and partners.

HPE SecureMail Blackberry for Microsoft® Exchange allows your mobile workforce to stay in contact—anytime, anywhere—using their corporate BlackBerry devices and without giving up secure communications. With HPE SecureMail Blackberry for Microsoft Exchange, all secure messages sent to and received by corporate Blackberry devices behave like standard email, without users going through any other steps. Outbound messages are automatically encrypted as they leave, and inbound messages are automatically decrypted as they enter the BlackBerry environment, securing email end-to-end. HPE Security Voltage outstrips its competition by integrating the HPE SecureMail for BlackBerry directly with BlackBerry Enterprise Server. This eliminates any need for additional device-level software or user training. All encryption and decryption activities are performed at the Blackberry Enterprise Server—and are completely transparent to internal users.

HPE Identity-Based Encryption for applications and websites that rely on email

HPE SecureMail Application Edition provides enterprises with a simple, yet powerful Web Services API for interacting with HPE Identity-Based Encryption (IBE) capabilities over HTTPS. The API is a REST-style Web service used to construct email encryption and decryption requests from within a number of different applications and websites that generate, store, and use email. Enterprises can use HPE SecureMail Application Edition to protect email from within a number of different applications and websites that generate, store, and use email. HPE SecureMail Application Edition extends data protection into application and website-driven business processes, while avoiding the complexity and cost associated with integrating secure email with applications (e.g., adding to the mail infrastructure, re-routing mail flows, and SDK-level integrations). Also included is the option to integrate with application and website business processes and workflows via HPE SecureMail SMTP interfaces.

Deliver secure statements directly to the user’s inbox

HPE SecureMail Statements Edition allows you to deliver automatically generated invoices, account information, and other electronic statements mailed in bulk directly to each customer’s inbox as a secure private email. The solution dramatically reduces the costs of printed statements delivered via snail mail or by courier (i.e., production, mail float, lost claims, etc.), and enhances the effectiveness of electronic statements delivered via online portals. The added data-level protection, ease of use, and convenience results in greater percentage of customer recipients.

Index and search messages in Symantec Enterprise Vault

HPE SecureMail Archive Connector automatically decrypts all secure email when they are archived to the Symantec Enterprise Vault, allowing easy indexing and full text searches of decrypted email in the archive. Other vendors' products require archive integration, plus they require the creation and management of additional keys for any type of review. This adds unneeded complexity to the process and can keep archives from being useful. But with the Symantec-certified archive connector, HPE SecureMail lets important workflows continue, with no additional administrative burden. Essential eDiscovery processes like collection, processing, review, and analysis can be conducted on decrypted messages, while keeping the highest-level security.

Support your eDiscovery Process

HPE SecureMail eDiscovery Accelerator offers supervisory access. It allows policy-controlled decryption of all secure emails in a user's mailbox—helping with easy indexing and full text searches. During the eDiscovery process, other vendors' products will miss all encrypted email stored locally on a user's system or in an email inbox. This places a huge burden on the IT staff to maintain compliance with regulatory agencies. The HPE SecureMail eDiscovery Accelerator solves this problem by making every secure email visible to an authorized supervisor during eDiscovery processes. HPE SecureMail eDiscovery Accelerator allows administrators to implement important workflows seamlessly throughout the organization, while upholding the highest levels of security.

Deliver large file attachments

Today, one of the big issues facing businesses is the need to exchange large files and collaborative information quickly and simply. Email message-size policies set by the sending and receiving organizations are often out of line with business needs. HPE SecureMail Large Attachment Delivery allows all messages with attachments of any size to be sent and received. The sender and the recipient don't need to take any special steps. When the recipient opens the secure email and clicks on the attachment link, the attachment is downloaded to the recipient—with no change in the user experience. HPE SecureMail Large Attachment Delivery facilitates business while eliminating the need for users to rely on unsecure Web-based file exchanges for critical data interchange, while improving productivity and eliminating help desk calls due to large blocked messages.

Easily encrypt files and documents

HPE SecureFile provides persistent data-level protection for sensitive and confidential data inside files and documents. HPE SecureFile is the only solution that effectively combats today's sophisticated data threats, while ensuring that people and applications can easily access the data—under policy control when they need it. HPE SecureFile offers a number of advanced capabilities not available with competing encryption products, such as tight integration with Microsoft Windows®, Active Directory, Exchange, and Office. Unauthorized access to documents and files remains one of the most commonly reported reasons for data breach incidents such as data loss and theft. HPE SecureFile adds a encryption button to Microsoft Office applications for simple encryption of documents from within Office applications. And the right-click menu adds a simple one-click encryption experience for any type of files supported on Windows. Integration with the Outlook and Exchange Address Book enables users to set and manage file access permissions (owner, editor, and viewer) for individuals and distribution lists. For example, you can let one user only read the contents of a document, let another user make changes to the document, and let another user manage file access permissions for other users.

Protect keys via Hardware Security Modules

HPE SecureMail supports the use of Thales nShield Connect Hardware Security Modules (HSMs). In this configuration, the HPE Identity-Based Encryption base secret and the user keys are generated inside a tamper resistant HSMs. District cryptographics for existing districts and newly created districts can also be protected by the HSM. HPE SecureMail also offers support for Operator Card Set (OCS)—providing additional layers of security for unattended/remote operation scenarios. HPE SecureMail enables businesses to comply with legal, regulatory, or policy requirements for secure, hardware-based key generation and protection.

Learn more at
voltage.com
hpe.com/software/datasecurity

Hewlett Packard
Enterprise